ABSTRACT

A secure method of authenticating an identification card, etc. The card is produced with a picture of anything desired on it along with the signature of the holder of the card, and digital copies of the photograph and signature are made. Certain pixels in the digital photograph and signature are chosen according to a characteristic value function algorithm, which can vary from card to card, and their values are recorded on the card, preferably on a magnetic strip, along with the cardholder's name and instructions for starting the authentication process. The digital photograph and signature are stored in a first remote location, and the characteristic value function algorithm is stored in a secure second remote location along with a digital processor. When the card is presented for authentication, the person to whom it is presented swipes it in a magnetic card reader. The cardholder's name and the pixel values are sent to the first remote location, and then sent along with the digital copies of the photograph and signature to the secure second remote location. The digital processor then uses the characteristic value function algorithm to determine the pixel values from the digital photograph and signature. If these match the values that were sent to it the card is declared authentic.

Counterfeiting such a card requires that someone hack into two locations, the one containing the characteristic value function algorithm and the one containing the digital photograph and signature, and insert material into each one. This increases the security of the entire system by considerably more than a factor of 2.